IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Michel A. Maillard et al.	Art Unit :	2136
Serial No.:	09/622,137	Examiner :	B. Hoffman
Filed :	August 11, 2000	Confirmation No.:	8272
Title :	METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED DIGITAL DATA		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION PURSUANT TO 37 CFR § 1.131

In connection with the Applicant's Response to the final Office Action of December 28, 2004, this Declaration sets forth the pertinent facts proving conception of the claimed invention prior to **January 28, 1998**.

1. We, Michel A. Maillard and Christian Benardeau, are the listed inventors for U.S. Patent Application 09/622,137 entitled "Method and Apparatus for Recording of Encrypted Digital Data."
2. We, Michel A. Maillard and Christian Benardeau, conceived the claimed invention prior to at least January 28, 1998 as evidenced by the enclosed document entitled "Protection Des Enregistrements Avec Mediabox" and (i) dated July 21, 1997, (ii) authored by Christian Benardeau, and (iii) setting forth a description of the claimed invention.
3. We, Michel A. Maillard and Christian Benardeau, conceived the claimed invention prior to at least January 28, 1998, as discussed above, in France.

4. We, Michel Maillard and Christian Benardeau, diligently worked on the reduction to practice of the invention from at least the date established by the enclosed document (referenced above) until at least the date of constructive reduction to practice established by the filing of European Patent Application 98400344.2 on February 13, 1998.

We, Michel Maillard and Christian Benardeau, hereby declare that all statements made herein of our own knowledge are true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Signed this day, 21 March of February 2005. _____
Michel Maillard

Signed this day, _____ of February 2005. _____
Christian Benardeau

Respectfully submitted,

Date: _____

_____
Jonathan P. Osha, Reg. No. 33,986
OSHA & MAY L.L.P.
1221 McKinney Street, Suite 2800
Houston, Texas 77010
Telephone: (713) 228-8600
Facsimile: (713) 228-8778

91097_1

4. We, Michel Maillard and Christian Benardeau, diligently worked on the reduction to practice of the invention from at least the date established by the enclosed document (referenced above) until at least the date of constructive reduction to practice established by the filing of European Patent Application 98400344.2 on February 13, 1998.

We, Michel Maillard and Christian Benardeau, hereby declare that all statements made herein of our own knowledge are true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Signed this day, _____ of February 2005. _____
Michel Maillard

Signed this day, 27 of February 2005. _____
Christian Benardeau

Respectfully submitted,

Date: _____

_____
Jonathan P. Osha, Reg. No. 33,986
OSHA & MAY L.L.P.
1221 McKinney Street, Suite 2800
Houston, Texas 77010
Telephone: (713) 228-8600
Facsimile: (713) 228-8778

91097_1

PROTECTION DES ENREGISTREMENTS AVEC MEDIABOX

Auteur : Christian Bénardeau

Date : 21 juillet 1997

Date d'impression : 21/07/97 08:33:21

Version : 01

FR 031189

Introduction

La diffusion d'événements sportifs exceptionnels ou de films récemment sortis en salle incitent les téléspectateurs à les enregistrer et à construire une vidéothèque. Cette constatation est d'autant plus vraie lorsqu'il s'agit d'émissions diffusées en numérique étant donné la qualité du son et de l'image.
Le fait de pouvoir enregistrer des émissions de qualité numérique sur des supports numériques tels que le mini disque de Sony ou la cassette SVHS de Philips ont donné des idées aux pirates. En effet, ils ont vite compris qu'en dupliquant les enregistrements, un énorme commerce parallèle pouvait se mettre en place. Ce commerce dans le domaine de télévision numérique à péage va rapidement devenir un manque à gagner important pour les Ayants Droits. Mais plus grave encore serait avec l'avènement d'Internet, une personne qui mettrait à disposition l'intégralité d'un enregistrement à l'ensemble des internautes de la planète.

Le but de ce document est de proposer une solution ouverte à tous les systèmes de contrôle d'accès pour éviter le piratage qu'il soit physique ou informatique en associant les supports d'enregistrement au système de contrôle d'accès Mediaguard développé par la Société Européenne de Contrôle d'Accès.

1. Contraintes et objectifs techniques.

Le dispositif utilisé pour la réception et l'enregistrement d'émission en matière de télévision numérique à péage, est constitué en général de trois éléments principaux:

- un décodeur rattaché à un contrôle d'accès.
- un lecteur de support d'enregistrement dit lecteur dans la suite de ce document
- un support d'enregistrement

La liaison entre le décodeur et le lecteur est du type IEEE 1394. Elle devra être impérativement chiffrée pour interdire aux pirates de la connecter directement à un PC par exemple.
L'enregistrement devra être chiffré de façon à interdire toutes copies physiques et tout échange entre abonnés pour ne pas léser les Ayants Droits. Pour cela, il paraît indispensable d'associer le lecteur à un composant cryptologique.
Enfin, le mot de contrôle ne devra jamais apparaître en clair dans la chaîne.

2. Enregistrement d'une émission.

Lorsque le décodeur reçoit une émission destinée à être enregistrer, il envoie l'ECM chiffré par la clé d'exploitation mensuelle au dispositif de sécurité contenu dans le lecteur. Ce dispositif extrait de l'ECM, le diversifiant mensuel et déchiffre l'ECM par le même procédé que l'Administration.
Puis, le dispositif de sécurité rechiffre l'ECM avec une clé aléatoire diversifiée par le numéro de série du lecteur. Dés lors, l'ECM est rattaché définitivement au lecteur.

Ce nouvel ECM est ensuite enregistré sur le support en même temps que les données qui lui sont associées.
Le dispositif de sécurité du lecteur formate aussi un message de type EMM dans lequel il insère la clé déterminée aléatoirement diversifiée par le numéro de série du lecteur ainsi que tous les critères d'accès (coût, séance,...) de l'émission enregistrée. Cet EMM est enregistré sur le support en même temps que les données si rattachant.

Dés lors, il ne reste plus au lecteur d'enregistrement à transmettre les enregistrements directement à la carte à puce du terminal lors de la lecture du support (EMM,ECM,data)

FR 031191

CANAL+

SOCIETE EUROPEENNE
DE CONTROLE D'ACCES

PROTECTION DES ENREGISTREMENTS

Division	**Direction Technique**
Département	**Cryptologie**
Date de création	21 Janvier 1998
Date de modification	23 Janvier 1998
Document	

FR 031221

HISTORIQUE

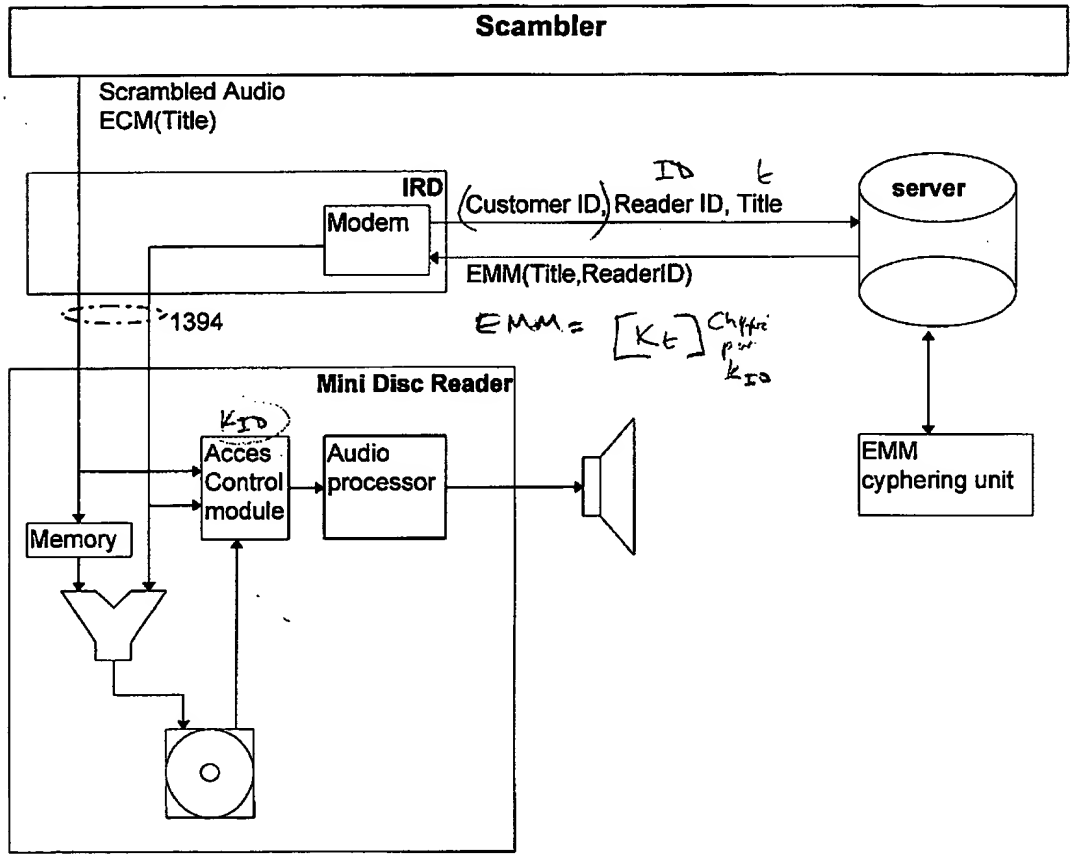
Edition	Date	Auteurs	Observations
1	*21 Janvier 1998*	Michel MAILLARD	Création.

FR 031222

1. MODULE INTÉGRÉ À L'ENREGISTREUR

1.1 Diffusion cyclique.

Chaque séquence audio est diffusée en boucle et insérée avec ses ECM dans le flux MPEG. Plusieurs titres peuvent être diffusé simultanément en fonction du débit disponible. Les données audio sont chiffrées à l'aide des mots de contrôle générés de façon aléatoire. Ces mots de contrôle sont transmis dans des ECM chiffrés par une clé diversifiée par la référence du titre.



Synoptique

HEADER Data	EMM (Title,ReaderID)	Audio Data ECM	Audio Data ECM		Audio Data ECM

Structure des données d'un titre

Enregistrement d'un titre :

1. Le client connecte sont enregistreur de mini-disque au terminal via l'interface 1394.
2. Le client sélectionne et paie un titre en utilisant l'application SONY en service dans terminal.

FR 031223

3. Le terminal envoie les données suivantes par MODEM : la référence du client, La référence du lecteur de mini-disque(information véhiculée par l'interface 1394), La référence du titre acheté.
4. Le serveur constitue un EMM qui contient la clé d'exploitation diversifiée par la référence du titre.
5. EMM est chiffré par l'unité de chiffrement en utilisant une clé diversifiée par la référence de l'enregistreur de mini-disque. $K_{ID}(K_E)$
6. Le terminal envoie alors l'EMM pour qu'il soit enregistré sur le mini-disque en début de titre.
7. Le terminal envoie directement les données audio et les ECM sans les déchiffrer.
8. Les données et l'ECM sont enregistrées directement sur le mini-disque. (Pour gagner du temps, il n'est pas nécessaire d'attendre le début du morceau pour démarrer l'enregistrement. Le collage des deux morceaux est réalisé par le lecteur).

Le client peut aussi commander par téléphone ou Minitel, dans ce cas l'EMM est transmis au centre de diffusion et inséré dans le multiplex MPEG. Le terminal doit connaître les références de l'enregistreur afin de pouvoir extraire l'EMM.

Lecture d'un titre :

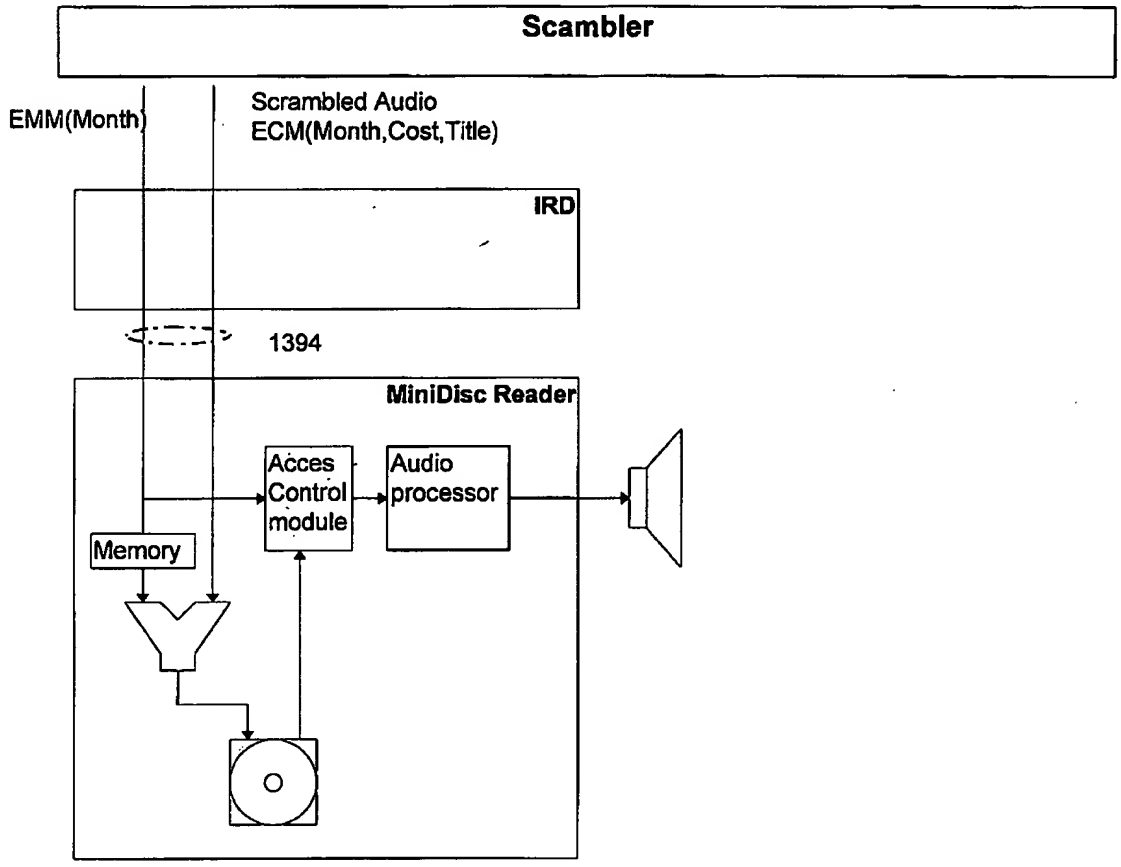
1. L'EMM enregistré au début du titre est envoyé au module de sécurité, Après déchiffrement la clé d'exploitation du titre est enregistrée dans la mémoire RAM du module de sécurité.
2. L'audio est déchiffré par le module de sécurité grâce aux ECM enregistrés.

Propriété :

Si la séquence audio est diffusée de manière cyclique le client peut commencer l'enregistrement de la séquence à n'importe quel moment, ou recommencer en cas de problème. Plusieurs clients peuvent enregistrer le même titre en même temps. Le titre n'est lisible que sur un lecteur. L'interface 1394 ne véhicule que des données chiffrées. Chaque titre contient l'ensemble des données de désembrouillage. Le module de sécurité ne garde pas en mémoire de donnée propre à chaque titres. Le client peut aussi commander par téléphone ou Minitel, dans ce cas l'EMM est transmis au centre de diffusion et inséré dans le multiplex MPEG. Le terminal doit connaître les références de l'enregistreur afin de pouvoir extraire l'EMM.

1.2 Achat en mode jeton

Chaque séquence audio est diffusée en boucle et inséré avec ses ECM dans le flux MPEG. Plusieurs titres peuvent être diffusé simultanément en fonction du débit disponible. Les données audio sont chiffrées à l'aide des mots de contrôle générés de façon aléatoire. Les mots de contrôle sont transmis associés à un coût dans des ECM chiffrés par une clé diversifiée par le numéro de mois en cours.



Synoptique

HEADER Data	EMM (ReaderID,Month)	Audio Data ECM	Audio Data ECM		Audio Data ECM

Structure des données d'un titre

Enregistrement d'un titre :

1. Le porte-monnaie intégré dans le module de sécurité doit contenir suffisamment de jeton pour permettre l'achat. Dans le cas contraire le client doit demander un chargement de jeton (par modem, téléphone ou Minitel).

FR 031225

2. L'enregistreur doit être connecté suffisamment à l'avance pour pouvoir mémoriser les EMM en cours de diffusion concernant le module de sécurité (30 minutes).
3. Le terminal sélectionne l'audio et les ECM et les envoie à l'enregistreur de mini-disque.
4. Sur demande du client L'ECM est envoyé au module de sécurité qui réalise l'achat. Un droit permanent est alors enregistré dans la mémoire EEPROM du module de sécurité.
5. L'enregistreur écrit sur le mini-disque les EMM en début de titre.
6. Les données et ECM sont enregistrées directement sur le minidisque. (Pour gagner du temps, il n'est pas nécessaire d'attendre le début du morceau pour démarrer l'enregistrement. Le collage des deux morceaux est réalisé par le lecteur).

Lecture d'un titre :

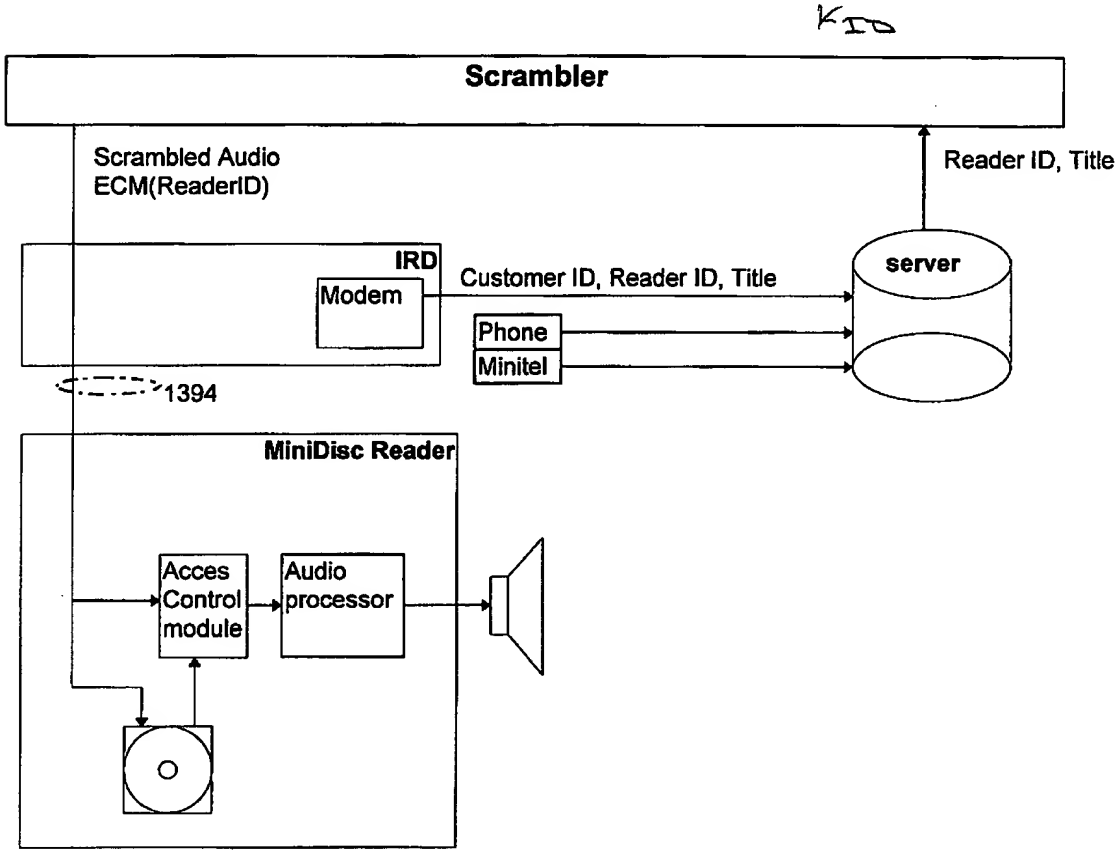
1. Les EMM placés au début du titre sont envoyés au module de sécurité, Ces EMM permettent le rechargement de la clé d'exploitation.
2. L'audio est déchiffré par le module de sécurité grâce aux ECM et après vérification des droits contenus dans le module de sécurité.

Propriété :

Si la séquence audio est diffusée de manière cyclique le client peut commencer l'enregistrement de la séquence à n'importe quel moment, ou recommencer en cas de problème. Plusieurs clients peuvent enregistrer le même titre en même temps. Le minidisque n'est lisible que sur un seul lecteur. L'interface 1394 ne véhicule que des données chiffrées. Chaque disque contient l'ensemble des données de désembrouillage. Un module de sécurité de 4000 octets d'EEPROM permet le stockage d'environ 1000 titres. Le faite de reconduire les modules de sécurité permet d'interdire l'enregistrement sur des lecteurs volés. La suppression des EMM est possible que si la clé d 'exploitation est fixe, le système devient alors plus vulnérable.

1.3 Diffusion à la demande

La séquence audio est diffusée une ou deux fois à chaque demande d'un client. Plusieurs titres peuvent être diffusé simultanément en fonction du débit disponible. Les données audio sont chiffrées à l'aide des mots de contrôle générés de façon aléatoire. Ces mots de contrôle sont transmis dans des ECM chiffrés par une clé diversifiée par la référence du module de sécurité du mini-disque du client.



Synoptique

HEADER Data	Audio Data ECM	Audio Data ECM		Audio Data ECM

Structure des données d'un titre

Enregistrement d'un titre :

1. Le client connecte sont enregistreur de mini-disque au terminal via l'interface 1394.
2. Le client sélectionne et pale un titre en utilisant l'application SONY en service dans terminal.
3. Le terminal envoie les données suivantes par MODEM : la référence du client, La référence du lecteur enregistreur de mini-disque(fournit par le client si la base de données distante ne la connaît pas), La référence du titre acheté.
4. Les données sont acheminées vers le codeur via le serveur de communication.

FR 031227

5. Le codeur fabrique des ECM chiffrés par une clé d'exploitation diversifiée par la référence du module de sécurité du mini-disque.
6. Le terminal envoie directement les données audio et les ECM sans les déchiffrer.
7. Les données et ECM sont enregistrées directement sur le minidisque. (Pour gagner du temps, il n'est pas nécessaire d'attendre le début du morceau pour démarrer l'enregistrement. Le collage des deux morceaux est réalisé par le lecteur).

Lecture d'un titre :

1. L'audio est déchiffré par le module de sécurité grâce aux ECM et après vérification des droits contenus dans le module de sécurité

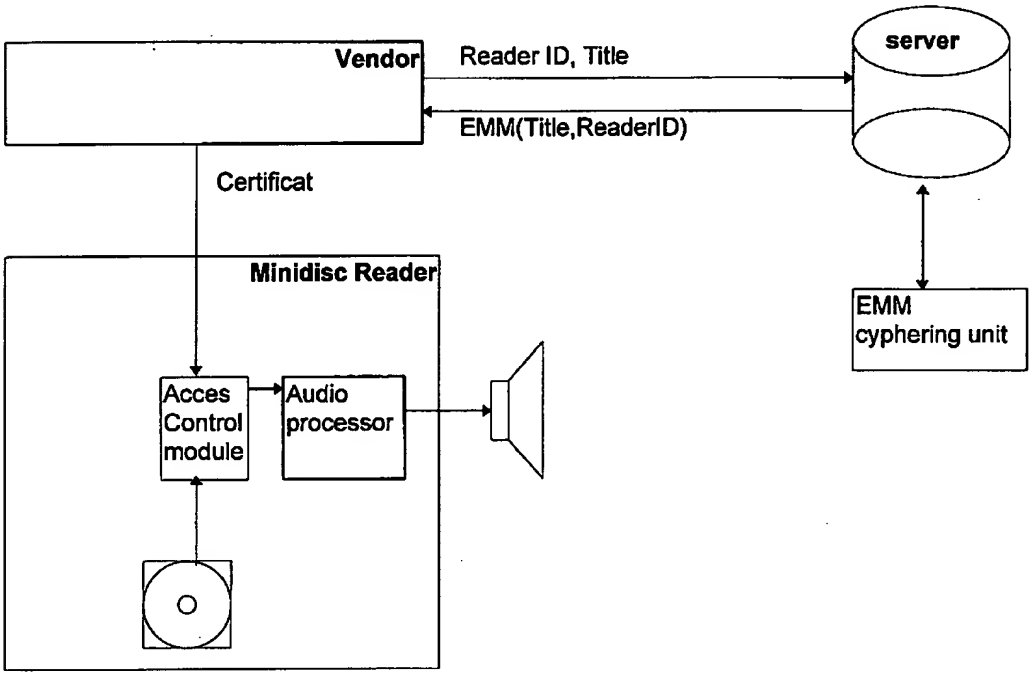
Propriété :

Le client doit préparer l'enregistreur de mini-disque avant de passer sa commande. En cas d'échec le client doit demander une rediffusion. Le minidisque n'est lisible que sur un lecteur. L'interface 1394 ne véhicule que des données chiffrées. Chaque titre contient l'ensemble des données de désembrouillage. Le client peut aussi commander par téléphone ou minitel, dans ce cas l'EMM est transmis au centre de diffusion et insérer dans le multiplex MPEG. Le module de sécurité utilise une clé chargée à la personnalisation.

1.4 MINI-DISQUE PREENREGISTREMENT

Les mini-disques sont fabriqués en série et sont donc tous identiques. Une partie ou la totalité des données sont chiffrées par une clé diversifiée par la référence du minidisque. La sécurité repose sur la génération d'un certificat généré à partir du numéro de série du lecteur de mini-disque lors de l'achat par le client. Le certificat peut être composé d'une clé de 40 bits minimum (12 chiffres décimal) associée à chaque titre.

Kt



Synoptique

HEADER Data	EMM (ReaderID,Title)	Audio Data ECM	Audio Data ECM		Audio Data ECM

Structure des données d'un titre

Achat du minidisque :

1. Le client achète un minidisque.
2. Le vendeur insère de disque dans un système de personnalisation. Le client indique la référence du lecteur de mini-disque.
3. Le système distant calcul un certificat contenant la clé de chiffrement du mini-disque. Le certificat est chiffré par une clé diversifiée par le numéro de série du lecteur (Le certificat peut être calculé en local à l'aide d'une carte mère) .
4. Le certificat est transmis au lecteur et est enregistré par le module de sécurité.

FR 031229

Transfert du certificat :

1. Le certificat peut être directement enregistré sur le mini-disque par le vendeur (si le disque le permet ?). Le certificat est transmis à chaque lecture. Le module de sécurité n'a pas besoin de mémoriser le certificat dans de la mémoire EEPROM.
2. Le certificat imprimé sous la forme d 'un code à bar par le vendeur en même temps que le ticket de caisse. Le certificat est collé sur le boîtier du mini-disque. Le certificat est transmis au module de sécurité par lecture optique.
3. Le certificat est transmis au module de sécurité par la connexion 1394 du lecteur directement chez le vendeur. Dans ce cas le client doit apporter le lecteur chez le vendeur.

Propriété :

Le certificat n'est utilisable que sur un seul lecteur. Si le client possède plusieurs lecteurs, il peut demander plusieurs certificats. Un module de sécurité de 4000 octets d'EEPROM permet le stockage d'environ 300 certificats. Si la lecture du code bar se fait directement de manière automatiquement à chaque insertion du mini-disque le module de sécurité n'a plus besoin de mémoriser les certificats.

2. MODULE DE SÉCURITÉ

mémoire EEPROM	Nb de bytes	diffusion cyclique	Mode jeton	à la demande	Préenregistré
Numéro de série	8	x	x	x	x
Clé de gestion diversifiée par numéro de série	8	x	x		x
Numéro unique (groupe+position)	4		x		
Clé diversifiée par numéro de groupe	8		x		
Clé d'exploitation du mois en cours	8		x		
Clé d'exploitation du mois suivant	8		x		
Clé d'exploitation diversifiée par numéro unique	8			x	
Clé d'exploitation constante	8		x		
Porte-monnaie	12		x		
Titre	N*4		x		
Certificat(Titre + clé)	N*12				x

Total pour 1000 titres		16	4064	16	12016

FR 031231

PROTECTING RECORDINGS WITH MEDIABOX

Author: Christian Bénardeau

Date: July 21, 1997

Printing Date: 7/21/97 8:33:21

Version: 01

Introduction

The broadcasting of special sports events or recently released films moves viewers to record them and build a video library. This is particularly true when these are digital broadcasts, given the quality of the sound and images.
Being able to record digital quality broadcasts on digital media like the Sony mini-disk or the SVHS cassette from Philips have given ideas to pirates. In fact, they have quickly understood that by duplicating recordings, an enormous black market could be established.
This market in digital pay-TV will rapidly become a significant failure to gain for Copyright holders. But what would be even more serious with the arrival of the Internet would be a person who would make a recording available to all Internet users in the world.

The purpose of this document is to propose an open solution to all access control solutions to prevent piracy, whether physical or electronic, by combining the recording media with the Mediaguard access control system developed by Société Européenne de Contrôle d'Accès.

1. Technical constraints and objectives

The device used to receive and record a digital pay-TV broadcast consists, in general, of three principal components:

- a decoder attached to an access control
- a recording media reader, called the reader in the rest of this document
- a recording medium.

The link between the decoder and the reader is the IEEE 1394 type. It must be coded to prevent pirates from connecting directly to a PC, for example.
The recording must be encoded in such a way as to prohibit any physical copies and any exchange among subscribers to avoid infringing on the rights of copyright holders. To achieve this, it appears vital to combine the reader with a cryptological component.
Finally, the password must never appear clearly in the chain.

2. Recording a broadcast

When the decoder receives a broadcast intended to be recorded, it sends the encoded ECM through the monthly operating key to the security element in the reader. This device extracts the ECM, the monthly diversifier and decodes the ECM using the same process as the Administration.
Then, the security device recodes the ECM with a random key diversified by the serial number of the reader. Then, the ECM is definitively attached to the reader.

This new ECM is then recorded on the medium at the same time as the data associated with it.
The security device of the reader also formats an EMM type message in which it inserts the randomly determined key diversified by the serial number of the reader along with all access criteria (cost, session, etc.) of the broadcast recorded. This EMM is recorded on the medium at the same time as the attached data.

At that one, the recording reader only has to transmit the recordings directly to the terminal smart card during the reading of the medium (EMM, ECM, data).